**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software

Encryption is the application of an algorithm to a section of text so that it cannot be read by people who don’t have the decryption key.

* 1. What are the two types of modern encryption methods?

The two types of modern methods of encryption are symmetric-key encryption and asymmetric-key encryption.

1. Network policies, profiles

Network policies and profiles refer to having an administrator of an organisation’s information system restrict the data that employees can access, relative to their security levels. Typically a username and password are required to access the data.

1. Firewalls

Firewalls are another type of restriction of access by outsiders to a network which is based on a combination of hardware/software that will only allow authorised network traffic to pass through the ‘gate’ that the firewall protects.

1. Antivirus software

Antivirus software is used to prevent computer virus infections. This software detects the presence of viruses as the computer boots up, when files are executed and when files are downloaded from the internet.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.

Security considerations for communications within an organisation are well documented processes for communicating sensitive information via email, telephone and fax. Use of passwords on documents that have sensitive information. Well documented policy for the use of the networked devices within the organisation.

**Storage**

1. **Filenaming conventions**
   1. List the 3 types of information each document should include.

Each document should include a date stamp (when the file was created and last saved), variation (identifying the version of the file is saved – version three or final copy, etc.), and name (something meaningful to identify the document).

* 1. Give an example of a sequential file-naming convention.

‘Newsletter 2011-11 030Oct’ - the name includes the date in which it is created, and the dates are listed in order.

1. **Location of files**

A directory can be set up to structure control of where documents are saved on the system so that they may be easily found again.

1. **Backups**
   1. Distinguish between each of the following:
      1. Full backup

Copies all the files from a device to storage medium. Takes considerable time and usually performed once a fortnight.

* + 1. Differential backup

Copies only the files which have been changed since the last back up. Restoring would involve restoring first the full back up and then the differential to restore files that have been changed since the last full back up.

* + 1. Incremental backup

Uses more than two backup media and also copies only the files which have been changed since the last full restore.

1. **Backup timeline**
   1. List good practice in relation to backup timelines.

It is good practice to clearly label all backup media so that you know when the backup was made and what it is on. A log may be kept by a systems manager recording backup dates, the location of backup files and whether any restorations have been made.

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

It is good practice to have multiple copies of data backed up on separate hard drives, which are located both onsite and offsite so that if one area is affected in an emergency, the other location will still have the backed up data.

* 1. What is the grandparent-parent-child system?

The grandparent-parent-child system refers to an incremental backup which is oerformed each day on separate tapes. The previous days tape becomes the generation above as a more recent version is created.

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

Archiving is the process of storing files to long term storage, then deleting from the hard disk, whereas destruction involves deletion only – the files are no longer saved.

* 1. What is a problem for ICT managers?

A problem for ICT managers is deciding which is the most appropriate long term storage media to use for backing up data.

* 1. What is a legacy system?

A legacy system is an old system which might run old databases on old servers or mainframes.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

When disposing information, organisations must consider issues of protecting data sensitive data, and how to properly delete the data so that it cannot be accessed by unauthorised people.